National Infrastructure Protection Center
CyberNotes

Issue #2001-15 *July 30, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between July 11 and July 27, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3Com[1]	Multiple	SuperStack II PS Hub 40	A vulnerability exists in certain models of 3Com hubs because the devices fail to restrict the allowed number of login attempts to the built-in Telnet based administration interface, which could let a remote malicious user cause a Denial of Service and/or use brute-force techniques to obtain access to the config accounts.	No workaround or patch available at time of publishing.	TelnetD Weak Password Protection	Low/ Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[1] CSC Sentry Research Labs, July 12, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
AdCycle.com[2]	Windows NT 4.0/2000, Unix	Adcycle 0.77, 0.77b, 0.78b, 1.0-1.5	A vulnerability exists because user input is not properly validated, which could let a remote malicious user bypass the administrator password check and gain administrator access.	Upgrade available at: http://www.adcycle.com/	AdCycle AdLogin.pm Admin Authentication Bypass	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Caldera[3]	Unix	OpenLinux Server 3.1, OpenLinux Workstation 3.1	An argument validation vulnerability exists in one of the CGI scripts, which could let a remote malicious user execute arbitrary commands.	Update available at: ftp://ftp.caldera.com/pub/updates/OpenLinux/3.1/Server/current/RPMS/docview-1.0-15.i386.rpm	OpenLinux DocView Meta-Character Filtering	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Check Point Software Technol-ogies[4] ***Proof of concept code released[5]***	**Multiple**	**Firewall-1 4.1 SP2 Build 41716, 4.1 Build 41439, 4.1**	**A directory traversal vulnerability exists which could let a remote malicious user pass packets across the firewall via port 259 by using false RDP (Reliable Data Protocol) headers on UDP packets. This makes it possible for remote users to gain access to restricted information systems. Not only can such access be gained with a Trojan horse that uses this vulnerability to connect from the inside back to the machine of the attacker, but also arbitrary connections from the outside to machines behind the firewall (even if they are supposedly totally blocked from inside and outside by the firewall) can be established.**	**Hotfix available at: http://www.checkpoint.com/techsupport/downloads.html**	**Firewall-1 RDP Header Firewall Bypassing**	**High**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.** ***Exploit code has been published.***
CheckPoint Software Technol-ogies[6]	Multiple	Firewall-1 4.0, 4.1 SP1-SP4	A vulnerability exists in the default settings because network topology information is sent to SecureRemote connections prior to authentication, which could let a remote malicious user gain sensitive information.	Patch available at: http://www.checkpoint.com/techsupport/downloads_sr.html	Firewall-1 SecureRemote Network Information Leak	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Cisco Systems[7]	Multiple	IOS 12.0-12.2	A Denial of Service vulnerability exists when a large number of UDP packets are sent to a device running IOS.	No workaround or patch available at time of publishing.	IOS UDP Denial of Service	Low	Bug discussed in newsgroups and websites.

[2] qDefense Advisory Number QDAV-2001-7-2, July 13, 2001.
[3] Caldera International, Inc. Security Advisory, CSSA-2001-026.0, July 17, 2001.
[4] Inside Security GmbH Vulnerability Notification, Revision 1.2, July 9, 2001.
[5] Bugtraq, July 13, 2001.
[6] Securiteam, July 18, 2001.
[7] Bugtraq, July 25, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
FreeBSD[8]	Unix	LBL tcpdump 3.6.2	A vulnerability exists in the way AFS packet headers are handled, which could let a remote malicious user execute arbitrary code as root.	Patch available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-01:48/tcpdump-4.x.patc	TCPDump AFS Signed Integer Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
GNU[9]	Unix	Groff 1.10, 1.11a, 1.14-1.16	A vulnerability exists in the groff utility used to process images, 'pic', which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Linux Groff Exploitation via lpd	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Hewlett-Packard[10]	Unix	HP-UX 10.20, 11.0, 11.11	A vulnerability exists in the login(1) command, which could let a malicious user circumvent security checks, traverse the local filesystem, and execute arbitrary programs.	Patches available at: PHCO_23900, PHCO_24083, PHCO_24267 http://itrc.hp.com	HP-UX Login Restricted Shell Escaping	**High**	Bug discussed in newsgroups and websites.
Hewlett-Packard[11]	Unix	HP-UX 11.11	A vulnerability exists in the Dynamically Loadable Kernel Module (dlkm) functionality, which could let a malicious user execute arbitrary code.	Upgrade available at: PHCO_23492 http://itrc.hp.com	HP-UX Dynamically Loadable Kernel Modules	**High**	Bug discussed in newsgroups and websites.
Hewlett-Packard[12]	Unix	VirtualVault 4.0, 4.5	A vulnerability exists in the /sbin/mkacct program because it incorrectly performs its functions, which could let a malicious user gain elevated privileges.	Upgrade available at: PHSS_24212 PHSS_24169 http://itrc.hp.com	HP VirtualVault MKACCT Privilege Elevation	Medium	Bug discussed in newsgroups and websites.
Horde[13]	Multiple	Horde Imp 2.0-2.2.5	Multiple vulnerabilities exist: 1. A remote malicious user could trick the server into fetching scripts from another host and then execute them; 2. A malicious user can execute malicious JavaScript code in the browser of an user who is reading an e-mail sent with special “javascript:” encodings; 3. A malicious user could make the server read a file called “prefs.lang” and execute it as PHP code.	Upgrade available at: ftp://atualizacoes.conectiva.com.br	Horde IMP Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites.
IBM[14]	Windows 9x/NT, OS/2, Unix	alphaWorks TFTP Server 1.21	A directory traversal vulnerability exists which could let a remote malicious user gain sensitive information.	No workaround or patch available at time of publishing.	alphaWorks TFTP Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[8] FreeBSD Security Advisory, FreeBSD-SA-01:48, July 17, 2001.
[9] Bugtraq, July 27, 2001.
[10] Hewlett-Packard Company Security Bulletin, 0160, July 17, 2001.
[11] Hewlett-Packard Company Security Bulletin, 0159, July 17, 2001.
[12] Hewlett-Packard Company Security Bulletin, 0161, July 19, 2001.
[13] Conectiva Linux Security Announcement, CLA-2001:410, July 25, 2001.
[14] Bugtraq, July 20, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[15]	Windows NT 4.0/2000, Unix	Tivoli SecureWay Policy Director 3.0.1, 3.6-3.7.1	A directory traversal vulnerability exists because the Web Seal Policy director does not handle URLs in hex code correctly, which could let a remote malicious user gain sensitive information.	Patch available at: ftp://ftp.tivoli.com/support/patches/	Tivoli SecureWay Policy Director Directory Traversal	Medium	Bug discussed in newsgroups and websites.
id Software[16]	Windows 95/98/NT 4.0	Quake 1.9	A Denial of Service vulnerability exists in the network play features.	No workaround or patch available at time of publishing.	Quake Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
id Software[17]	Windows 95/98/NT 4.0	Quake3 Arena 1.16n, 1.1.7	A remote Denial of Service vulnerability exists when a large number of forged client queries are generated.	No workaround or patch available at time of publishing.	Quake 3 "smurf attack" Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
IpSwitch[18]	Windows NT 4.0/2000	WS FTP Server 2.0-2.0.2	A buffer overflow vulnerability exists when the length of the argumenting string exceeds the size of its input buffer, which could let a malicious user execute arbitrary code with SYSTEM privileges.	Patch available at: http://www.ipswitch.com/cgi/download_eval.pl?product=WR-0000	WS-FTP Anonymous Multiple FTP Command Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Knox Software[19]	Unix	Arkeia Server 4.2.8-2	A vulnerability exists because sufficient file creation permissions are not used, which could let a malicious user gain elevated privileges.	No workaround or patch available at time of publishing.	Arkeia Backup World Writable File Creation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[20]	Windows 2000	Windows 2000 & 2000 SP1 & SP2	A vulnerability exists because Windows 2000 is not case sensitive when determining whether or not a process is associated with the OS or not. If a file has the same name as a critical system process, a user will not be able to terminate it, which could let a malicious program run on a system with out the possibility of it being terminated via Task Manager.	No workaround or patch available at time of publishing.	Windows 2000 Task Manager Process Termination	**High**	Bug discussed in newsgroups and websites.
Microsoft[21]	Windows 2000	Windows 2000, 2000 SP1 & SP2	A vulnerability exists in the implementation of the 'NetuserChangePassword' function, which could let a malicious user change network passwords.	No workaround or patch available at time of publishing.	Windows 2000 Unauthorized Password Change	Medium	Bug discussed in newsgroups and websites.

[15] iXsecurity Security Vulnerability Report, July 23, 2001.
[16] Bugtraq, July 16, 2001.
[17] Securiteam, July 24, 2001.
[18] Defcom Labs Advisory, def-2001-28, July 26, 2001.
[19] Bugtraq, July 23, 2001.
[20] Bugtraq, July 16, 2001.
[21] NTBugtraq, July 18, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[22]	Windows 95/98	Windows 95, 98	A vulnerability exists when specifying a path to a file containing spaces in the Windows Registry, which could let a malicious user execute arbitrary programs.	No workaround or patch available at time of publishing.	Windows 9x Quotation Exclusion File Execution	**High**	Bug discussed in newsgroups and websites.
Microsoft[23]	Windows NT 4.0/2000	Exchange Server 5.5, 2000; SQL Server 7.0, 2000; Windows NT 4.0, 2000	A remote Denial of Service vulnerability exists in several of the RPC servers associated with system services because inputs are not adequately validated.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-041.asp	Windows Malformed RPC Request Denial of Service CVE Name: CAN-2001-0509	Low	Bug discussed in newsgroups and websites.
Microsoft[24]	Windows NT 4.0/2000	Microsoft Services for Unix 2.0	Two Denial of Service vulnerabilities exist: a vulnerability in the Telnet services; and a vulnerability in the implementation of NFS.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-039.asp	Microsoft Services for Unix Telnet and NFS Denial of Service CVE Name: CAN-2001-0505	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[25]	Windows NT 4.0/2000	Windows 2000 Server, Windows NT 4.0, Terminal Server Edition	A Denial of Service vulnerability exists due to a memory leak in one of the functions that processes incoming Remote Data Protocol data via port 3389, and a flaw in the Terminal Server service.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-040.asp	Invalid RDP Data and Windows Terminal Server Denial of Service CVE Name: CAN-2001-0540	Low	Bug discussed in newsgroups and websites.
Microsoft[26]	Windows NT 4.0/2000	Windows Media Player 6.4, 7.0, 7.1	A buffer overflow vulnerability exists in the functionality used to process Windows Media Station, '.NSC', files, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-042.asp	Windows Media Player Buffer Overflow CVE Name: CAN-2001-0541	**High**	Bug discussed in newsgroups and websites.
Miro Construct Pty Ltd[27]	Multiple	Mambo Site Server 3.0-3.0.5	A vulnerability exists which could let a malicious user bypass the authentication mechanism and gain administrator privileges.	No workaround or patch available at time of publishing.	Mambo Site Server Administrator Password Bypass	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[22] Bugtraq, July 18, 2001.
[23] Microsoft Security Bulletin, MS01-041, July 27, 2001.
[24] Microsoft Security Bulletin, MS01-039, July 24, 2001.
[25] Microsoft Security Bulletin, MS01-040, July 25, 2001.
[26] Microsoft Security Bulletin, MS01-042, July 27, 2001.
[27] Securiteam, July 27, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[28]	Multiple	Baltimore Techno-logies MAIL Sweeper SMTP 4.2.1; F-Secure Anti-Virus 5.0.2, 5.2.1	A Denial of Service vulnerability exists because it is possible to construct an archive with an unusually high compression ratio, resulting in a small file that grows to extreme size when uncompressed.	No workaround or patch available at time of publishing.	Multiple Vendor File Scanner Malicious Archive Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the press and other public media.
Multiple Vendors[29]	Unix	BSDi BSD/OS 4.0-4.2; FreeBSD 2.x, 3.x, 4.0.x, FreeBSD 3.5.1, 4.1.1, 4.2 & 4.3 STABLE & RELEASE; NetBSD 1.0-1.5.1; Netkit Linux Netkit 0.10-0.12; OpenBSD 2.0-2.8; SGI IRIX 6.5; Sun Solaris 2.0-2.6, 7.0, 8.0	A buffer overflow vulnerability exists in Telnet daemons derived from BSD source code, which could let a remote malicious user crash the server and under certain circumstances gain root privileges.	**BSDi:** http://www.bsdi.com/services/support/patches/ **FreeBSD**: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-01:49/	Multiple Vendor Telnetd Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Multiple Vendors[30]	Unix	Conectiva 6.0, 7.0; RedHat Linux 7.0	A vulnerability exists because the 'Expect' program searches insecure directories for dynamic libraries, which could let a malicious user execute arbitrary code.	**Conectiva:** ftp://atualizacoes.conectiva.com.br/	Multiple Linux Vendor Expect Insecure Library Loading	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[31]	Unix	Conectiva 6.0, 7.0; RedHat Linux 7.0	A vulnerability exists in 'TCL/TK' (Tool Command Language/Toolkit) program, which could let a malicious user execute arbitrary code.	**Conectiva:** ftp://atualizacoes.conectiva.com.br/	Multiple Linux Vendor TCLTK Unsafe Library Searching	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[32]	Unix	Debian 2.1, 2.2; RedHat 6.1, 6.2, 7.0, 7.1; Slackware 7.0, 7.1, 8.0	A vulnerability exists in the 'man' program, which could let a malicious user create a cache file that will execute arbitrary code when another user views a manual page corresponding to that cache file.	No workaround or patch available at time of publishing.	Multiple Vendor Malicious Manual Page Cache File Creation	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[28] SecurityFocus, July 17, 2001.
[29] TESO Security Advisory, July 10, 2001.
[30] Conectiva Linux Security Announcement, CLA-2001:409, July 19, 2001.
[31] Conectiva Linux Security Announcement, CLA-2001:409, July 19, 2001.
[32] Securiteam, July 23, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[33]	Unix	Horde IMP 2.0, 2.2, 2.2.1- 2.2.5; Horde 1.2, 1.2.1	A vulnerability exists because Horde and Imp use /tmp in an unsafe manner and does not protect internal data files from being viewed by local/remote malicious users.	**Caldera:** ftp://ftp.caldera.com/pub/updates/OpenLinux/3.1/Server/current/RPMS/	Horde and Imp Temporary File	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[34]	Unix	Linux kernel 2.4.3-2.4.6	A vulnerability exists in the initialization scripts because they rely on inheriting a safe umask from 'init' and execute without setting it explicitly, which could let a malicious user gain root privileges.	No workaround or patch available at time of publishing.	Linux Init Default Umask	**High**	Bug discussed in newsgroups and websites. There is no exploit required.
Multiple Vendors[35]	Multiple	Softek MailMarshal 4.0-4.2; Trend Micro ScanMail 1.0	A vulnerability exists in the way restricted filetypes are handled as attachments, which could let a malicious user insert extraneous characters in the filename extension of a hostile attachment. The affected gateway will fail to detect the modified extension.	No workaround or patch available at time of publishing.	Multiple Vendor SMTP Attachment Protection Bypass	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Multiple Vendors[36, 37]	Unix	PHPLib Team PHPLIB 7.2-7.2.1	A vulnerability exists in the 'PHPLIB', which could let a remote malicious user execute arbitrary scripts.	http://sourceforge.net/project/showfiles.php?group_id=31885&release_id=44737 **Trustix:** ftp.trustix.net/pub/Trustix/updates **Conectiva:** ftp://atualizacoes.conectiva.com.br	Multiple Vendor 'PHPLIB' Remote Script Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[33] Caldera International, Inc. Security Advisory, CSSA-2001-025.0, July 19, 2001.
[34] Bugtraq, July 16, 2001.
[35] Securiteam, July 25, 2001
[36] Trustix Secure Linux Security Advisory #2001-0014, July 26, 2001.
[37] Conectiva Linux Security Announcement, CLA-2001:410, July 25, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[38]	Windows NT 4.0/2000, Unix	OpenLDAP 1.0-2.0.7; iPlanet Directory Server, version 5.0 Beta-4.13; Lotus Domino R5 Servers (Enterprise, Application, and Mail), prior to 5.0.7a; Teamware Office for Windows NT and Solaris, prior to version 5.3ed1; Qualcomm Eudora WorldMail for Windows NT ver. 2; Microsoft Exchange 5.5 LDAP Service; Network Associates PGP Keyserver 7.0, prior to Hotfix 2; Oracle 8i Enterprise Edition; IBM SecureWay Directory 3.0-3.2 Solaris, 3.0-3.2 Win2K	Several implementations of the Lightweight Directory Access Protocol (LDAP) protocol contain vulnerabilities, which could let a malicious user cause a Denial of Service, gain unauthorized privileged access, or both, or execute arbitrary code. For more information please see Cert Advisory located at: http://www.cert.org/advisories/CA-2001-18.html	Contact your vendor for a patch.	OpenLDAP Denial of Service	Low/ **High**	Bug discussed in newsgroups and websites. Vulnerabilities have appeared in the press and other public media.
Nathan Neulinger[39]	Unix	CGIWrap 1.0- 3.6.4	A vulnerability exists because CGIWrap does not filter embedded scripting commands from user-supplied input, which could let a malicious user execute arbitrary commands.	Upgrade available at: http://prdownloads.sourceforge.net/cgiwrap/cgiwrap-3.7.tar.gz	CGIWrap Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[38] CERT® Advisory CA-2001-18, July 19, 2001.
[39] Bugtraq, July 22, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NetBSD[40]	Unix	NetBSD 1.3-1.3.3, 1.4-1.4.3, 1.5, current pre20010701	A Denial of Service vulnerability exists due to insufficient length checking on the 'msg_controllen' member of the 'msghdr' structure.	Patch available at: ftp://ftp.netbsd.org/pub/NetBSD/security/patches/SA2001-011-sendmsg-1.3-1.5.patch **current pre20010701:** ftp://ftp.netbsd.org/pub/NetBSD/security/patches/SA2001-011-sendmsg-current.patch	NetBSD sendmsg Denial of Service	Low	Bug discussed in newsgroups and websites.
NetWin Limited[41]	Windows 95/98/NT 4.0/2000, MacOS 9.0, BSD/OS 4.0.1, Unix	SurgeFTP 1.0b, 2.0a, 2.0b; DMail 2.5d, 2.7, 2.7q, 2.7r, 2.8e-2.8i	Multiple vulnerabilities exist in the NetWin Authentication module (NWAuth): numerous buffer overflow vulnerabilities which could let a malicious user execute arbitrary code; and a weak password encryption vulnerability, which could let a malicious user decrypt the passwords.	No workaround or patch available at time of publishing.	NetWin NWAuth Buffer Overflow and Weak Password Encryption	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit script has been published for the Weak Encryption vulnerability.
Procmail[42]	Unix	Procmail 3.10, 3.11, 3.13, 3.14, 3.15	A race condition vulnerability exists in several signal handlers used by the program, which could let a malicious user interrupt a non-reentrant libc function and enter it again from the handler.	Update available at: ftp://updates.redhat.com/	Procmail Unsafe Signal Handling Race Condition	Medium	Bug discussed in newsgroups and websites.
RedHat[43]	Unix	Linux 7.1	A vulnerability exists in the 'vipw' program due to incorrectly set permissions of the '/etc/shadow' file after editing it, which could let a malicious user read its contents. This may lead to a system compromise.	Update available at: ftp://updates.redhat.com/7.1/en/os/	Vipw Insecure File Permissions	Medium/ **High**	Bug discussed in newsgroups and websites.
Richard Everitt[44]	Unix	Pileup 1.1	Two buffer overflow vulnerabilities exist due to insecurely structured calls to 'scanf', which could let a malicious user execute arbitrary code with root privileges.	Upgrade available at: http://www.securityfocus.com/data/vulnerabilities/patches/pileup-1.2.tar.gz	Pileup Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Sambar Technol-ogies[45]	Windows NT	Server 4.4 production. Server 5.0 beta1, beta2, beta3, beta4	A vulnerability exists which could let a remote malicious user craft a web request which will cause pagecount to overwrite existing files or create arbitrary files.	**Workaround:** Comment out the following line in your config.ini and restart your server: "INIT = samples.dll: general_init" **Upgrade available at:** http://www.sambar.com/	Sambar Server Pagecount File Overwrite	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[40] NetBSD Security Advisory, 2000-011, July 20, 2001.
[41] Securiteam, July 23, 2001.
[42] Red Hat, Inc. Red Hat Security Advisory, RHSA-2001:093-03, July 13, 2001.
[43] Red Hat, Inc. Red Hat Security Advisory, RHSA-2001:095-04, July 16, 2001.
[44] Bugtraq, July 22, 2001.
[45] Bugtraq, July 22, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sambar Technol-ogies[46]	Windows, Unix	Server 4.1 production through 4.4, Server 5.0 beta1-beta5	A vulnerability exists due to insecure default protection for user passwords, which could let a malicious user obtain sensitive information.	**Workaround:** Reconfigure Sambar to use a non-recoverable password protection format: In config.ini set Use Unix crypt = true DES encryption.	Sambar Server Insecure Default Password Protection	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Samsung[47]	Windows NT 4.0/2000, Unix	ml85p Printer Driver 1.0	A vulnerability exist because ml85p does not check for symbolic links when creating image output files, which could let a malicious user elevate his/her privileges.	No workaround or patch available at time of publishing.	ML85p Printer Utility Symlink	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Scott R. Lemmon[48]	Multiple	Proxomitron Naoko-4 beta1-beta4	A cross-site scripting vulnerability exists because of the way URLS are displayed in error messages, which could let a malicious user execute an arbitrary script.	Upgrade available at: http://spywaresucks.org/prox/beta.html	Proxomitron Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
Snapstream[49]	Windows	Personal Video Station 1.2a	Two vulnerabilities exist: a password storage vulnerability because passwords and user information are stored in plaintext; and a directory traversal vulnerability which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	Snapstream PVS Plaintext Password and Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sonic WALL[50]	Multiple	SOHO 4.0.0, 5.0.0, 5.1.5.0	A vulnerability exists in the TCP/IP stack implementation, which could let a malicious user predict the TCP initial sequence numbers.	No workaround or patch available at time of publishing.	SOHO Firewall Predictable TCP Initial Sequence Number	Medium	Bug discussed in newsgroups and websites.
SSH Communi-cations Security[51]	Unix	SSH2 3.0	A password authentication vulnerability exists when there are two or less characters in the password field, which could let a remote malicious user gain root access.	Update available at: ftp://ftp.ssh.com/pub/ssh/ssh-3.0.1.tar.gz	SSH Short Password Login	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[46] Bugtraq, July 25, 2001.
[47] Bugtraq, July 10, 2001.
[48] Bugtraq, July 24, 2001.
[49] Bugtraq, July 26, 2001.
[50] Bugtraq, July 25, 2001.
[51] Bugtraq, July 20, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Steve Grimm[52]	Unix	Un-CGI 1.0-1.9	Two vulnerabilities exist: a script access validation vulnerability because when Un-CGI executes scripts, it does so without checking to see if the executable bit is set which could let a remote malicious user gain access to the host; and a directory traversal vulnerability because user-supplied input is not properly filtered, which could let a malicious user gain sensitive information.	Upgrade available at: http://www.midwinter.com/~koreth/uncgi.html	Script Access Validation and Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro systems, Inc.[53]	Unix	Sun Solaris 2.6, 2.6_x86, 7.0,7.0_x86	A buffer overflow vulnerability exists in DTMail, which could let a malicious user execute arbitrary code.	Patch available at: http://sunsolve.sun.com/securitypatch	DTMail Environment Variable Buffer Overflow CVE Name: CAN-2001-0548	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Valerie Mates[54]	Unix	Interactive Story 1.3	A directory traversal vulnerability exists because '../' sequences from user input are not properly filtered when submitted to a hidden file called 'next', which could let a remote malicious user view sensitive information.	Update available at: http://www.valeriemates.com	Interactive Story Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
XFree[55]	Unix	XFree86 X11R6 3.3.2	A buffer overflow vulnerability exists in the way the MANPATH variable is handled by xman, which could let a malicious user execute arbitrary code and potentially gain root access.	No workaround or patch available at time of publishing.	XMan ManPath Environment Variable Buffer	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Zone Labs[56]	Windows 95/98/NT 4.0/2000	ZoneAlarm For Windows 95/98/2000 2.1, ZoneAlarm for Windows 95/98/2000 2.2-2.6, ZoneAlarm for Window NT 4.0 2.1-2.6	A vulnerability exists in the way long filenames are handled, which could let a malicious user bypass the MailSafe feature.	No workaround or patch available at time of publishing.	ZoneAlarm MailSafe Bypass	Medium	Bug discussed in newsgroups and websites.

*"Risk" is defined by CyberNotes in the following manner:

[52] Securiteam, July 24, 2001.
[53] NSFOCUS Security Advisory, SA2001-04, July 24, 2001.
[54] qDefense Advisory Number QDAV-2001-7-3, July 15, 2001.
[55] Bugtraq, July 11, 2001.
[56] Bugtraq, July 18, 2001.

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between July 10 and July27, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 45 scripts, programs, and net-news messages containing holes or exploits were identified. *At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 27, 2001	**Pic-lpr-remote.c**	**Script which exploits Remote Linux Groff Exploitation via lpd vulnerability.**
July 26, 2001	Ettercap-0.5.4.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
July 26, 2001	Ws_ftp.pl	Perl script which exploits the WS-FTP Anonymous Multiple FTP Command Buffer Overflow vulnerability.
July 25, 2001	Insidethreat.txt	Document which provides a basic understanding of how important it is to maintain security within the corporate network, and to offer some theory and techniques that the hacker (the insider) may use or may be using to penetrate vital systems within your organization.
July 25, 2001	Sadecrypt.zip	Exploit for the Sambar Server Insecure Default Password Protection vulnerability.
July 25, 2001	**Smtp-a-x.pl**	**Perl script which exploits the Multiple Vendor SMTP Attachment Protection Bypass vulnerability.**
July 24, 2001	Sol_sparc_dtmail_MAIL_ex.c	Script which exploits the Solaris DTMail Mail Environment Variable Buffer Overflow vulnerability.
July 23, 2001	**Attqt.pl**	**Script which exploits the Multiple Vendor SMTP Attachment Protection Bypass vulnerability.**

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 23, 2001	Getacct003.zip	GetAcct sidesteps "RestrictAnonymous=1" and acquires account information on Windows NT/2000 machines.
July 23, 2001	**Ida-exploit.sh**	**Script which exploits the Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow vulnerability.**
July 23, 2001	**Nwauthcrack.csites**	**Exploit for the NetWin NWAuth Buffer Overflow and Weak Password Encryption vulnerability.**
July 23, 2001	Scooplm003.zip	Searches out the password from LM/NTLM authentication information (LanManager and Windows NT challenge/response).
July 23, 2001	Spc002.zip	Share Password Checker acquires the list of shared folders of a Windows 95/98/Me machine on the network and shows you those folders' passwords. It uses the "Share Level Password" Vulnerability and checks whether the patch for this vulnerability has been applied to the target host.
July 22, 2001	Ae-gateway.tar.gz	A Man-in-the-Middle Gateway to assist sniffing in switched environments that forces itself to become an invisible intermediary gateway between the gateway and the victim host.
July 21, 2001	Pwl9x-0.04-dev.tar.gz	A program that will allow you to see the passwords contained in your Windows pwl database under Unix.
July 20, 2001	Mimedefang-1.3.tar.gz	A flexible MIME e-mail scanner that works with Sendmail 8.10 / 8.11 and will alter or delete various parts of a MIME message according to a flexible configuration file.
July 20, 2001	**Nmap-2.54BETA27.tgz**	**A utility for port scanning large networks.**
July 20, 2001	Snmpbrute-fixedup.c	A fast SNMP brute forcer that doesn't need to wait for a response.
July 20, 2001	Wfp-020-installshield.zip	Advanced remote Windows OS detection.
July 19, 2001	Complete3.htm	A textual guide for breaking into computer networks from the Internet that includes host enumeration, scanners, custom tools, protocols, windows information, and much more.
July 19, 2001	Kbdv3.c	A Linux loadable kernel module backdoor that allows root access by modifying the SYS_utime and SYS_getuid32 system calls.
July 19, 2001	Kis-0.9.tar.gz	A client / server LKM based rootkit.
July 19, 2001	Vippr1_1.2.tar.gz	Beta of a concept study of attack routers that is a userland virtual router that can be used together with any routing protocol attack tools.
July 18, 2001	Filter-xpl.c	Script which exploits the /usr/local/bin/filter vulnerability.
July 18, 2001	Ktv.sh	Local root exploit for the Ktvision v0.1.1-271 and below symlink vulnerability.
July 18, 2001	Libwhisker-pr3.tgz	A Perl module for performing whisker CGI vulnerability checks.
July 18, 2001	Qdav-2001-7-3	Exploit URL for the Interactive Story Directory Traversal vulnerability.
July 18, 2001	Sig.c	Script which exploits the FreeBSD 3.1 - 4.3 signal condition vulnerability.
July 18, 2001	Slackware.init.txt	Exploit for the Slackware 8.0 'modprobe lp' vulnerability.
July 18, 2001	Sneaky2.sh	A "Swiss army knife" for Hotmail/Messenger that implements spoofing/brute force/misconception/unexpected input class attacks.
July 18, 2001	Sr.pl	SecureRemote allows any IP to connect and download sensitive network information. This Perl script gives a potential attacker a wealth of information including IP addresses, network masks (and even friendly descriptions).
July 18, 2001	Ttawebtop.html	Exploit for the Tarantella 3.01 ttawebtop.cgi "show files" vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 17, 2001	**42.zip**	**Exploit for the Multiple Vendor File Scanner Malicious Archive Denial of Service vulnerability.**
July 17, 2001	Aldebaran-3.0.1.tar.gz	An advanced libpcap-based network TCP, UDP, and ARP network sniffer that gives a user captured data and basic information about addresses and ports.
July 17, 2001	Ethereal-0.8.19.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
July 17, 2001	Log_analysis-0.38.tar.gz	A log file analyzer, which extracts relevant data for any of the recognized log messages and produces a summary.
July 17, 2001	**Ml85p.sh**	**Exploit for the ML85p Printer Utility Symlink vulnerability.**
July 17, 2001	Slackware.man.c	Script which exploits the Slackware 8.0 and below symlink vulnerability.
July 17, 2001	**Xxman.sh**	**Exploit for the XMan ManPath Environment Variable Buffer vulnerability.**
July 16, 2001	Netscript-1.6.3.tgz	A portable TCP socket scripting tool.
July 16, 2001	**Qflood.c**	**Script which exploits the Id Software Quake Denial of Service and Quake 3 "smurf attack" Denial of Service vulnerabilities.**
July 13, 2001	Fw1_bypass_rdp.c	Script which exploits the Firewall-1 RDP Header Firewall Bypassing vulnerability.
July 12, 2001	**3comcrack.pl**	**Perl script which exploits the 3Com TelnetD Weak Password Protection vulnerability.**
July 10, 2001	**Ml85pexploit.c**	**Script which exploits the ML85p Printer Utility Symlink vulnerability.**
July 10, 2001	**Ml85pexploit2.c**	**Script which exploits the ML85p Printer Utility Symlink vulnerability.**

Trends

Probes/Scans:

- **There has been an increase in scans of port 23 probing for the Multiple Vendor TelnetD vulnerability. (For more information, see the Multiple Vendor Telnetd Buffer Overflow vulnerability described above.)**
- **CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.**

Other:

- **Internet backbone providers have notified the NIPC they are witnessing large-scale victimized web servers scanning for Microsoft Internet Information Server (IIS) vulnerabilities. The activity of the Code Red worm has the potential to degrade services running on the Internet. Any web server running the Microsoft IIS versions 4.0 or 5.0 that is not patched is susceptible to infection and exploitation as an attack platform. The NIPC is strongly urging consumers running these versions of IIS 4.0/5.0 to check their systems and install the patch. For more information, see NIPC ADVISORY 01-015, located at: http://www.nipc.gov/warnings/advisories/2001/01-015.htm or NIPC ALERT 01-016, located at http://www.nipc.gov/warnings/alerts/2001/01-016.htm. The Microsoft bulletin describing this vulnerability and its patch to fix the problem may be found at: http://www.microsoft.com/technet/security/bulletin/MS01-033.asp (also in CyberNotes-2001-13). Also see Trojan Section "TROJ_BADY.A."**
- **CERT/CC has received reports of W32/Sircam from over 300 individual sites. "W32/Sircam" is malicious code that spreads through e-mail and potentially through unprotected network shares. Once the malicious code has been executed on a system, it may reveal or delete sensitive information. (See Trojan Section). For more information, see CERT® Advisory CA-2001-22,**

located at: http://www.cert.org/advisories/CA-2001-22.html. Also see Trojan Section, "TROJ_SIRCAM.A".

- **This year there has been a significant increase in activity resulting in compromises of home user machines. In many cases, these machines are then used by intruders to launch attacks against other organizations. For more information, see CERT® Advisory CA-2001-20, located at: http://www.cert.org/advisories/CA-2001-20.html.**
- A bogus Microsoft Bulletin spreads the Internet worm, W32.Leave.B.Worm.
- Two network-aware viruses, PE_Funlove.4099 and PE_Magistr.A, have resurfaced and are spreading at a rapid rate.
- **The NIPC and FedCIRC have recently received information on attempts to locate, obtain control of and plant new malicious code known as "W32-Leaves.worm" on computers previously infected with the SubSeven Trojan. For more information, see ADVISORY 01-014, located at: http://www.nipc.gov/warnings/advisories/2001/01-014.htm.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

Ranking	Common Name	Type of Code	Trends	Date
1	W32/SirCam	Worm	New to Table	July 2001
2	W32/Magistr	File, Worm	Stable	March 2001
3	W32/Hybris	Worm	Slight Decrease	November 2000
4	W32/BadTrans	Worm	Slight Increase	April 2001
5	PE_MTX.A	File Infector, Trojan	Slight Decrease	September 2000
6	VBS/Loveletter	Script	Increase	March 2000
7	W32/Funlove	File	Slight Increase	November 1999
8	VBS/Homepage	Script	Decrease	May 2001
9	VBS/Kakworm	Script	Slight Decrease	December 1999
10	VBS/Stages	Script	Return to Table	June 2000

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **213** distinct viruses are currently considered “in the wild” by anti-virus experts, with another **485** viruses suspected. “In the wild” viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Bat.Count.A.273 (Virus): This is the batch file that is dropped by the VBS.Count.A.int worm. It deletes all files in the C:\, C:\Windows, C:\Documenti, and C:\Programming folders.

ce8.476 (File Infector Virus): The virus is a small memory-resident, .com file infecting virus that uses encryption on its virus code. Infected files have their file size increased by 476 bytes.

Thirteen Minutes (DOS Virus): This is a old DOS memory resident virus that infects .com files. After that, whenever the victim executes or opens any .com file, the virus will infect that file by appending 712 bytes to it.

VBS.Cable (Visual Basic Script Worm): This worm attempts to connect to a computer at an IP address, and then tries to write to that computer's hard drive. However, this is successful only if the drive that it is trying to write to is a shared drive. If the worm does connect to a shared drive, it attempts to remove files (if they exist) that were placed on that computer by another virus and replace them with copies of its own Trojan horse program. The worm copies both itself and the file Sys32.exe to the shared drive. Both files are copied into the \StartUp\ folder so that they will run automatically the next time that Windows starts.

VBS_CATFISH.A (Aliases: CATFISH.A, CATFISH, VBS.Catfish@mm) (Visual Basic Script Virus): This worm propagates via Microsoft Outlook, MIRC and PIRCH. In Outlook it sends itself as an attachment, CATFISH.BAT, to all addresses listed in an infected user's address book. For MIRC or PIRCH users, it sends the CATFISH.HTML file to all users connected to the same channel as the infected user. It also drops a CATFISH8ME.VBS file and a CATFISH.HTML file in the Windows directory. This worm is unstable, and due to bugs in its code, it does not execute properly. It has no destructive payload.

VBS.Count.A.int (Visual Basic Script Worm): This worm spreads by using Microsoft Outlook. It adds a value to the registry and drops a VBS file that, if run, drops a .bat file that deletes all files in the C:\, C:\Windows, C:\Documenti, and C:\Programmi folders.

VBS/LoveLet-CZ (Visual Basic Script Worm): This is a variant of the VBS/LoveLet-AS Visual Basic Script worm. The worm forwards itself as an e-mail attachment with the subject line "US PRESIDENT AND FBI SECRETS =PLEASE VISIT => (http://WWW.2600.COM)<=" or a random 6 letter string. The e-mail message body will either be "VERY JOKE..! SEE PRESIDENT AND FBI TOP SECRET PICTURE.." or a random 10 letter string. Running the attached file infects your computer. On 17 September, the worm displays a message box containing the text "Dedicated to my best brother=>Christiam Julian(C.J.G.S.) Att. TEGIF (M.H.M. Team)" where 'TEGIF' can be any random 5 letters. It then attempts to disconnect drives Z: through to E:. The worm creates a copy of itself in the System directory with a filename of 5-8 characters with the extension .BMP.vbs, .asf.vbs or .JPG.vbs. It is this file which is mailed out to all addresses in the infected user's Outlook address book.

VBS.Merlin.B@mm (Aliases: VBS.Eva@mm, VBS.Merlin.A@mm) (Visual Basic Script Worm): This is a mass-mailing worm that spreads by e-mailing itself to all contacts in the Microsoft Outlook address book. It can also spread across network drives and by using an IRC client. Its main payload creates 2,500 randomly-named folders in the root of drive C and places a text file in each of these folders. It is able to infect Microsoft Word template files, overwrite .exe files, and delete Windows system files.

VBS.XPJunexp.intd (Aliases: VBS.Yang@mm, I-Worm.Yang (Visual Basic Script Worm): This worm contains a bug that prohibits it from replicating. The bug is trivial to fix and for that reason the write-up is aimed at providing information about the functionality of this worm when the bug is fixed For this worm to replicate, the operating system must be Windows XP or the Microsoft Outlook 2000 View Control must be installed. It sends itself out to all recipients in the victim's Microsoft Outlook address book, and it overwrites all files that have ht in their extension (such as .htm and .html).

W32.Antiqfx.C.Worm (Alias: Win32.HLLW.AntiQFX.b(Win32 Worm): This is a minor variant of the W32.Antiqfx.Worm. They differ only in the size of the worm program. Both variants have identical behavior. W32.Antiqfx.C.Worm also propagates over the network. The payload deletes files of a specific type and file name.

W32.HLLO.Videoinf (W32 Worm): This is a virus that overwrites .ht* and .exe files in the folder that it is executed from. It sends information from the computer on which it is run to an e-mail address. On certain dates, the virus will modify the C:\Autoexec.bat file so that the hard drive will be formatted when the computer is restarted.

W32.Pet_Tick.G (Alias: W32.Malot.int) (Win32 Worm): This is a mass-mailing worm. It infects all .html files in the \Windows folder, sends country information that it finds in the Win.ini file to the virus's author, and sends copies of the worm to mailto: addresses that it finds in the cache folder of Internet Explorer. It may also modify the Win.ini file.

W97M.Shore.J (Alias: W97M.Shore) Word 97 Macro Virus): This is a Microsoft Word macro virus that infects the global template, Normal.dot, and spreads when files are opened, closed, saved, or when exiting Word. The virus disables the Visual Basic Editor within Microsoft Word by requiring a password to access it.

W97M.Tester.A (Word 97 Macro Virus): This is a Microsoft Word macro virus that spreads by infecting Microsoft Word documents and the global template, Normal.dot. The virus attempts to decrease the security level of Microsoft Word 97, 2000, and XP.

W97M.Thus.EY (Word 97 Macro Virus): This is a simple Macro Virus that infects Word documents when then are opened, closed, or when a new document is created.

W97M.Zeitung.A (Alias: W97M.Zeitung) (Word 97 Macro Virus): This is a Microsoft Word macro virus that spreads by infecting Microsoft Word documents and the global template, Normal.dot. Documents infected by this virus may occasionally cause Word to display an error message when the documents are opened, even though the virus is still able to replicate.

WM97/Marker-C (Word 97 Macro Virus): This virus has been reported in the wild. It is a variant of the WM97/Marker-A Word macro virus. Whenever a document is closed, the virus FTPs user information from Word to the Codebreakers site and appends this information to the bottom of the macro as comments.

WM97/Marker-GT (Word 97 Macro Virus): This is a corrupted but viable variant of the WM97/Marker-C Word macro virus. Whenever a document is closed, the virus attempts to FTP information about the infected user from Word to a website belonging to the Codebreakers hacking group. It also appends this information to the bottom of the macro as comments.

WM97/Marker-GU (Word 97 Macro Virus): This is a corrupted but viable variant of the WM97/Marker-C Word macro virus. Whenever a document is closed, the virus attempts to FTP information about the infected user from Word to a website belonging to the Codebreakers hacking group. It also appends this information to the bottom of the macro as comments.

WM97/Quiet-F (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents and the global NORMAL.DOT template file. The virus contains no deliberately malicious payload.

WM97/Thus-EP (Word 97 Macro Virus): This is a member of the WM97/Thus Word macro virus family. The virus does not contain a harmful payload, and infects documents when they are opened or when new documents are created.

WM97/Thus-EZ (Word 97 MacroVirus): This is a member of the WM97/Thus Word macro virus family. The virus does not contain a harmful payload, and infects documents when they are opened or when new documents are created.

X97M_LAROUX.MV (Aliases: LAROUX, X97M/Laroux.dx.gen, LAROUX.MV) (Excel 97 Macro Virus): This virus has been reported in the wild. When an infected Excel file is opened, it copies itself to a RESULT.XLS file in the Excel startup directory. It intercepts the automacro Auto_Open so that after it has installed itself, it infects all documents that are opened. It inserts its user-defined macros at the start of infected files and its actual virus code at the end of the macro module. It does not re-infect files that contain its virus module RESULTS.

X97M_SLACKER.A (Aliases: SLACKER.A, X97M/SLACKER) (Excel 97 Macro Virus): This virus has been reported in the wild. It infects Excel documents that are opened or closed. Before it infects files, it deletes any code in the ThisWorkbook module. It has an empty payload (that does nothing) on the system date December 31, 2000 at 8:00 a.m.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
AOL.PWSteal.86016	N/A	CyberNotes-2001-14
Artic	0.6 beta	CyberNotes-2001-14
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Bionet.318	N/A	CyberNotes-2001-13
Backdoor.Bionet.40a	N/A	CyberNotes-2001-14
Backdoor.Darkirc	**N/A**	**Current Issue**
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	N/A	CyberNotes-2001-06
Backdoor.Quimera	N/A	CyberNotes-2001-06
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-JZ	N/A	CyberNotes-2001-02
Backdoor-QN	N/A	CyberNotes-2001-13
Backdoor-QO	N/A	CyberNotes-2001-13
Backdoor-QR	N/A	CyberNotes-2001-13
Backdoor-QT	N/A	CyberNotes-2001-14
Backdoor-QV	N/A	CyberNotes-2001-14
Backdoor-QZ	N/A	CyberNotes-2001-14
BAT.Black	N/A	CyberNotes-2001-11
Bat.FAGE.1482	**N/A**	**Current Issue**
Bat.Hexvirus.1414	**N/A**	**Current Issue**
BAT.Install.Trojan	N/A	CyberNotes-2001-04
Bat.PG94.3964	**N/A**	**Current Issue**
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
BAT_FORMATC.K	N/A	CyberNotes-2001-13
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07
DLer20.PWSTEAL	N/A	CyberNotes-2001-05
DMsetup.IRC.Worm	N/A	CyberNotes-2001-13
EIC.Trojan	N/A	CyberNotes-2001-14

Trojan	Version	CyberNotes Issue #
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Flor	N/A	CyberNotes-2001-02
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
Goga	N/A	CyberNotes-2001-12
HardLock.618	N/A	CyberNotes-2001-04
Jammer Killah	1.2	CyberNotes-2001-10
JAVA_STORM.A	N/A	CyberNotes-2001-13
JS.StartPage	N/A	CyberNotes-2001-07
JS_ZOPA.A	N/A	CyberNotes-2001-14
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
PWSteal.Trojan.D	N/A	CyberNotes-2001-13
SadCase.Trojan	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
SennaSpy Generator	N/A	CyberNotes-2001-13
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
Troj/PsychwardB	N/A	CyberNotes-2001-14
Troj/Slack	N/A	CyberNotes-2001-14
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BADY	**N/A**	**Current Issue**
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAFEIN111.A	N/A	CyberNotes-2001-14
TROJ_CAINABEL151	1.51	CyberNotes-2001-06
TROJ_CHOKE.A	N/A	CyberNotes-2001-13
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IDENTD.B	N/A	CyberNotes-2001-11

Trojan	Version	CyberNotes Issue #
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_IRC_NETOL.A	N/A	CyberNotes-2001-14
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_LATINUS.SVR	N/A	CyberNotes-2001-12
TROJ_LEAVE.A	N/A	CyberNotes-2001-13
TROJ_LINONG.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.B	N/A	CyberNotes-2001-13
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MEGA.A	N/A	CyberNotes-2001-12
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	N/A	CyberNotes-2001-12
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_NEWSFLOOD.A	N/A	CyberNotes-2001-13
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_PSW.GINA.A	N/A	CyberNotes-2001-13
TROJ_Q2001	N/A	CyberNotes-2001-06
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SIRCAM.A	**N/A**	**Current Issue**
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	.22	CyberNotes-2001-06
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	2.2	CyberNotes-2001-06
TROJ_SUB722_SIN	N/A	CyberNotes-2001-06
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_VAMP.A	N/A	CyberNotes-2001-13
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_WARHOME.A	N/A	CyberNotes-2001-12
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
Trojan.Assault.10	**10**	**Current Issue**
Trojan.Billrus.Texto	N/A	CyberNotes-2001-14
Trojan.Diagcfg	**N/A**	**Current Issue**
Trojan.Lornuke	N/A	CyberNotes-2001-14
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.RASDialer	N/A	CyberNotes-2001-06
Trojan.Sheehy	N/A	CyberNotes-2001-05

Trojan	Version	CyberNotes Issue #
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.VBS.PWStroy	N/A	CyberNotes-2001-14
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.Blank.A	N/A	CyberNotes-2001-14
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.Phybre	N/A	CyberNotes-2001-12
VBS.Reset	N/A	CyberNotes-2001-12
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.BatmanTroj	N/A	CyberNotes-2001-04
W32.BrainProtect	N/A	CyberNotes-2001-07
W32.Leave.B.Worm	N/A	CyberNotes-2001-14
Y3K Rat	1.6	CyberNotes-2001-11

Backdoor.Darkirc: This backdoor Trojan horse gives unauthorized people access to a compromised computer, and it has the functionality to activate a WWW, IRC, FTP or SMTP server on the victim's computer.

Bat.Hexvirus.1414: This is a batch file Trojan. It attempts to drop two files; the first file turns the second file into an executable file that carries the possibly destructive payload. Due to bugs in the code, the virus does not succeed in infecting the computer, but it does cause the computer to stop responding.

Bat.PG94.3964: This is a batch file Trojan that includes comments from the author. It adds itself to the top of any batch file that is located in the same folder as the virus. The virus checks to see if it has been run as the file Pg94.bat, (instead of Pg94). Infected batch files have their file sizes increased by 703 bytes and run noticeably slower.

Bat.FAGE.1482 (Aliases: Bat.Duke.1432, Bat.damn.1432): This is a batch file Trojan that drops an executable file, $.com. Due to bugs in the virus code, when it is executed the dropped file causes the computer to stop responding. The virus attempts to use the dropped file on all batch files on the system except for Autoexec.bat.

Trojan.Assault.10 (Aliases: Flooder.Win32.Assault.10, FDOS/Assault.10): This Trojan can be used to flood a single IP address with packets of data. When executed, the program displays a simple interface that allows a hacker to configure the program to flood a victim. A victim's IP address is entered, and the hacker can then choose which port to flood, how many packets to send, the size of the packets to send, and how many packets to send per second. These packets can be sent using either User Datagram Protocol (UDP) or Internet Control Message Protocol (ICMP).

TROJ_BADY (Aliases: CODERED.A, CODE RED, HBC, W32/Bady.worm): This Trojan has been reported in the wild. It uses a remote buffer overflow vulnerability in Internet Information Service (IIS) Web servers that can give system-level privileges to a remote user, thereby compromising network security. The Microsoft bulletin describing this vulnerability and its patch to fix the problem may be found at: http://www.microsoft.com/technet/security/bulletin/MS01-033.asp. This worm has two trigger dates and two payloads. The first payload is triggered when the current system date is between 20 and 28. The worm executes a distributed denial of service attack (DDoS) on a government Web site (www1.whitehouse.gov). The second payload is triggered if the current system date is less than 20. The payload then executes and generates random IP addresses and sends copies of itself through port 80.

Trojan.Diagcfg: This Trojan modifies the registry so that it loads whenever Windows is started. It listens on port 6967 for commands and sends e-mail to its creator with information about the computer's IP address and connected hosts. If the program is run again while it is already running, it displays the misleading message: “This program is part of the system and can not be run separately”.

TROJ_SIRCAM.A (Aliases: SCAM.A, TROJ_SCAM.A, W32.Sircam.Worm@mm): This Trojan has been reported in the wild. It is a high-level program created in Delphi that propagates via e-mail using SMTP commands. The Trojan arrives as an e-mail attachment with two extension names (i.e., ,FNAME.EX1.EX2). FNAME.EX1 is a random file chosen from an infected user's personal folder, referred to in the below entry:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Personal

EX2 can have a .LNK, .EXE, .COM, .BAT or .PIF filename. The e-mail arrives in English or Spanish. The attachment is a copy of the worm merged with a randomly chosen file from the sender's computer. When opened, it copies the worm to hidden files, SCAM32.EXE in the System directory and SIRC32.EXE in the Recycled folder. The worm modifies the below to execute at every Windows startup:

HKLM\Software\Microsoft\Windows\CurrentVersion\
RunServicesDriver32=“%systemdir%\Scam32.exe”

It modifies the below to execute when an .EXE file is run:

HKCR\exefile\shell\open\command=“”C:\Recycled\SirC32.exe” ”%1” %*

It also creates the below registry where it stores its data:

HKLM\Software\SirCam

To hide its malicious activities, it extracts the appended host file to the Temp and Recycled folders, then opens it with the default application it is associated with (.DOC with MS Word or Wordpad, .XLS with MS Excel, .ZIP with WinZip). The Temp folder varies depending on a computer’s setting. Infected users may use the “set” command in the command prompt to check this folder's actual path. The worm then searches for files containing e-mail addresses such as .WAB (Windows Address Book) and .HTM, and sends e-mails to the addresses. The host file appended at the end of the worm may contain a .DOC, .XLS, or .ZIP file that is taken from a folder specified in the below entry:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Personal

It saves the path and filename of host files to the SCD.DLL file and the e-mail addresses it gathered to SC??.DLL files (i.e., SCI1.DLL and SCW1.DLL), all hidden and saved in the Systemdir (C:\Windows\System) directory. The worm file stores in the registry the number of e-mail addresses gathered. To propagate, it tries to connect to the server that sent an infected e-mail. If it fails, it tries to connect to three other e-mail servers whose addresses are stored within the worm body and which are random in nature. Upon connection, it uses a stored list of SMTP commands to create and send mail over the Internet. To infect via shared drives, it lists all existing connections. If it finds a folder with write access, it searches for and copies itself to SIRC32.EXE in the Recycled folder. If it finds an AUTOEXEC.BAT file in the folder, it opens this and appends: @win\recyled\sirc32.exe. It searches the shared folder for a Windows directory, then copies RUNDLL32.EXE to RUN32.EXE and itself to RUNDLL32.EXE. When a computer is infected via the network, it activates only upon reboot. NT-based OSes are safe from this type of attack. Occasionally, it copies itself to files other than SIRC32.EXE, SCAM32.EXE, or RUNDLL32.EXE. When executed, it deletes all files and folders in the system. Not all files in the default Windows folder are erased since some may currently be in use.